ANALYST BRIEF

Cybercrime Kill Chain vs. Defense Effectiveness

SUBVERSION OF LAYERED SECURITY

Authors – Stefan Frei, PhD; Francisco Artes

Overview

Global Internet penetration and e-commerce have grown explosively over the past two decades. It is currently estimated, as of 2012, that more than two billion users have Internet access.[1] With the ongoing deployment of information technology, comprehending the evolution of information security at large has become much more than the mere understanding of the underlying technologies. There is a growing realization that security failures are caused as often by bad incentives and awareness as by bad design or neglected implementation of available security technologies - while cybercriminals continue to surprise defenders with new attack methodologies and innovative evasion techniques to bypass detection.

This brief first examines the attacker's kill chain; the main tracks from the external attacker to the target, which lead to the compromise of the victim's server or desktop machine. Defense in depth, on the other hand, represents the use of multiple security techniques to help mitigate the risk of one component of the defense being compromised or circumvented. In the second part of this paper, we examine the four major classes of protection technologies (firewall, intrusion prevention systems, endpoint protection/antivirus, browser protection) that large organizations typically deploy and rely upon. Empirical data will be layered to present results on the security effectiveness of these protection technologies as measured in NSS Labs' group tests. Each class of technology tested is represented by the leading products from that product group. The products are subjected to an array of the industry's most rigorous testing procedures including load and stability, live malware, known and unpublished exploits, and diverse evasion techniques.

Generally, NSS finds a considerable gap in protection levels within and across different security product groups.

[1] Internet Word Stats - http://www.internetworldstats.com/stats.htm

NSS Labs Findings

- Vendor claims on the effectiveness or performance of their products are frequently found to be overly optimistic, or based on unrealistic assumptions that do not apply to real-world deployments.
- The general availability of malware tools leads to an increase in opportunistic attacks.
- Automated vulnerability scanners and attack tools cannot determine whether or not your enterprise should consider itself a high-risk target.
- Antivirus does not prevent a dedicated attacker from compromising a target.
- Three of the six tested network firewall products tested crashed when subjected to NSS' stability tests.
- IPS evasion detection has improved considerably from 2009 to 2012.
- IPS products failed to detect in between 17 to 334 of 1,486 exploits tested.
- Antivirus products differ up to 58 percent in effectiveness at stopping exploits, with protection levels varying between 34 percent and 92 percent. Several products failed detection of exploits when switching from HTTP to HTTPS.

NSS Labs Recommendations

- Enterprises should conduct a thorough risk assessment to determine whether they are high-risk targets. However, even low risk targets should assume they will be subject to opportunistic attacks at some point.
- A risk-based approach to IT security — identifying the systems and assets that are most vulnerable to attack and whose compromise would be most damaging to the enterprise — is crucial to defending against and remediating targeted persistent attacks (TPAs).
- High-risk enterprises should assume that they are already compromised – there is no product or combination of products that provides 100 percent protection.
- Organizations should complement prevention with breach detection and security incident and event monitoring (SIEM) to identify and act on successful security breaches in a timely manner.
- Utilize independent information on security product effectiveness and performance during product purchase, refresh, and upgrade cycles to make the right deployment decisions. In NSS tests, vendors' performance claims were frequently found to be excessively optimistic.

Analysis

Understanding the Enemy

Understanding the capabilities and motivation of the enemy is a crucial step in planning and executing any kind of defense. It is of paramount importance to first look at the changing threat environment, and then examine the attacker's "kill chain."

The Changing Threat Environment

In cybersecurity, the threat landscape has evolved considerably in the last decade. In a first order approximation, this evolution can be mapped on the two dimensions *expertise of the attacker* vs. *motivation of the attacker*, as shown in figure 1.

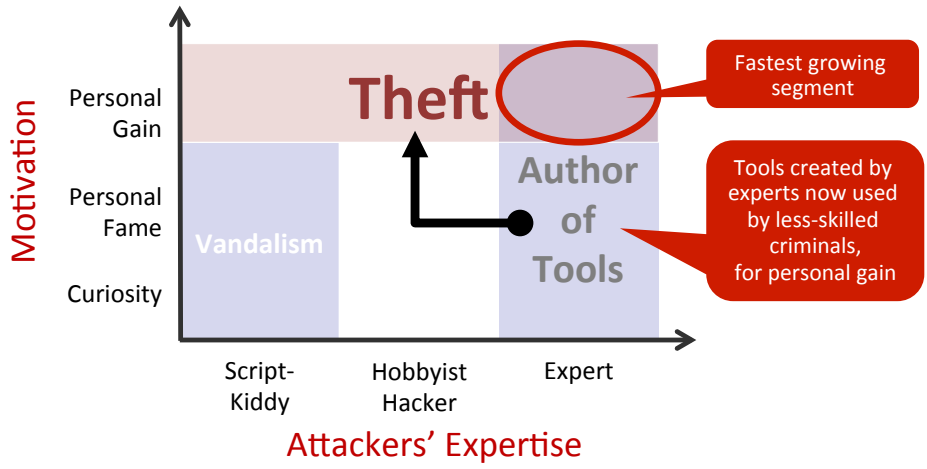

Figure 1 – Attacker's Expertise vs. Attacker's Motivation

Hobbyist attackers working out of curiosity or for personal fame are depicted in the lower left corner, classified as "vandalism." When profit-making is the goal, independent of the attackers expertise, the activity can be classified as criminal or theft, depicted on the top in Figure 1. In recent years, and motivated by profits, experts created an array of advanced commercial off-the-shelf (COTS) malware tools to automate their job. This evolution, paired with stiff competition within the cybercrime scene/industry, has resulted in the general availability of sophisticated malware tools at low prices. Such tools are readily available to anyone interested in starting a cybercrime career. Figure 2 shows a snapshot of a selection of tools commonly offered on the underground market. Depicted are tools to generate Trojans, modify existing malware in order to evade detection, automate the malware development processes, and quality-check the malware. Due to competition in the field, these tools are usually offered with comprehensive service and customer care packages. For example, exploit kits such as Blackhole have essentially made the mass exploitation of websites a low cost franchise operation with a low buy in and an immediate lucrative return.

Figure 2 – A Series of Malware Tools as Commonly Offered in the Underground

From the defender's point of view, this evolution of the threat landscape has the following implications:

- The availability of sophisticated malware tools results in a high degree of attack automation. This ranges from systematic identification of vulnerable targets to successive fully automated exploitation.
- The general availability of malware tools leads to an increase in opportunistic attacks, as the attacker no longer needs expertise or special skills.
- Expert know-how is developed and available. Enterprises should consider threat actors to be determined, highly skilled, and experts in the field.

The first two of the above arguments also demonstrate that any enterprise can become a victim of attack at any time, for any reason, and without being specifically targeted. Automated vulnerability scanners and attack tools cannot differentiate if an enterprise should consider itself a high-risk target or not, as they often are used to target a subnet or range of IP addresses.

The Attacker's Kill Chain

To successfully compromise a target, an external attacker executes a methodology as depicted in figure 3. The defender, on the other hand, tries first to prevent the attack, or detect the breach if prevention failed.

Figure 3 – Attacker's Basic Methodology – and Defender Options

After identification of the target, the attacker prepares the toolsets and malware to be used. Assuming the targeted organization has several layers of defense in place, the attacker modifies the malware used in order to evade detection. Cybercriminals have formidable knowledge about the weaknesses of diverse security products – gained through information exchange and thorough internal testing. It is a trivial exercise to determine the type of

security products deployed in the targeted organization. Passive information gathering, insiders, or ex-employees are common sources. Network scanning, analyzing e-mail probes, and mining public information such as social media and support forums also provide a wealth of information on the security defenses deployed. A determined attacker will only use malware that was successfully tested to bypass the expected defense technologies. After the attack bypasses detection, it exploits the target and starts executing the value extraction according to the attackers objective (espionage, fraud, etc.)

Anti-Evasion Strategies

In order to render defense technologies, especially signature-based technologies, ineffective a large number of serial variants, or permutations, of the core malware are created. Using off-the-shelf tools, hundreds of thousands of new malware samples can be created in less than an hour. While being functionally identical to the original malware, all samples look different to detection engines.

Following the creation, all samples will be subjected to a quality assurance process. The malware samples are tested against all major, up-to-date antivirus engines. Only samples that successfully pass this test (i.e. are not detected) are then used for deployment. Specialized services exist that allow cybercriminals to have all their samples continuously tested and be alerted by mail or text message if a sample is subsequently detected by a new signature. By the time of attack, the malware used by a dedicated attacker is known to be undetectable by common antivirus programs.

Further anti-evasion techniques can be applied, such as tunneling/encryption, use of different encodings, IP/RPC fragmentation, TCP segmentation, compression, or URL obfuscation to just name a few.

Failure to handle a particular type of evasion by a security device means an attacker can use an entire class of exploits for which the device is assumed to have protection, rendering it virtually useless. This is only compounded as the number of evasion techniques increases. It should be noted, however, that failing one evasion in all categories is considered worse then failing all evasions in a single category. For example, it is better to miss all techniques in one evasion category, such as HTTP URL obfuscation, than one technique in each category, which would result in a broader attack surface.

Furthermore, evasions operating at the lower layers of the network stack (IP fragmentation or TCP segmentation) result in a bigger impact on security than those operating at the upper layers (HTTP, FTP) because lower-level evasions impact a broader range of exploits. For example, a single RPC fragmentation evasion can be applied to more than 30 different remote Oracle Database attacks that would have been blocked by their respective signatures.

The test results presented in the next section of this brief document the efficacy of diverse anti-evasion techniques.

Attacker vs. Target Initiated

Since the mass adoption of firewalls, network address translation (NAT) at the gateway, and perimeter defense, not all targets can be reached directly by an external attacker. It is, therefore, important to differentiate between attacker-initiated and target-initiated attacks, as depicted in figure 4.

Attacker Initiated:

The attacker executes the threat remotely against a vulnerable application and/or operating system. These attacks traditionally target servers and the attack is executed completely under the control of the attacker. Typically, servers are single-purpose machines, optimized and hardened according to function, and run a few, but critical services, that are directly exposed to the Internet.

Target Initiated

The vulnerable target initiates the threat, typically by an end user opening a document containing malware or by clicking on a malicious link. The attacker has little or no control over when the target user or application will execute the threat. These attacks traditionally target a selection of the numerous client applications found on any desktop computer. Prevalent and frequently targeted applications include Adobe Flash & Reader, Firefox, Internet Explorer, Oracle/Sun Java, Office applications, QuickTime, etc. Despite being reachable only through indirect attacks, client desktops are increasingly the main focus of attack for threat actors. This is due to the large number and diversity of installed applications, each potentially vulnerable, paired with unpredictable usage patterns of human operators. Typical end-point systems were found to have more than 50 programs from more than 22 different vendors installed. This complexity results in a significant attack surface, and serves to highlight also the difficulty of keeping typical end-points up-to-date with security patches.

Effectiveness of Layered Defense

To be successful at penetrating a typical enterprise perimeter, an attacker must bypass several layers of defensive mechanisms. Organizations deploy an array of technologies in order to prevent attacks, or to detect the compromised systems as early as possible as shown in Figure 3. In this section we examine the following four core protection technologies typically deployed in organizations:

- Network firewall
- Intrusion prevention systems
- Endpoint protection/antivirus
- Web browser block protection

The boundary between different defense technologies and products has become increasingly blurred over the years. Further, some of the functionality can be deployed either on the network as an inline device, or as a host-based solution (e.g., network vs. host based IPS of firewall).

In figure 4, we illustrate attack paths from the intruder to the target with these principal protection layers. We do not discuss breach detection here. We further differentiate perimeter and host based protection.

- Firewalls and intrusion prevention systems (IPS) are typically deployed as centrally managed network appliances.
- Endpoint protection/antivirus and the browsers URL block protection is typically deployed on the target host (while still being centrally managed).

The common goal of these technologies is the prevention of attacks – to deny access to malicious traffic on the network level, or detect and prevent execution of malware on the host.

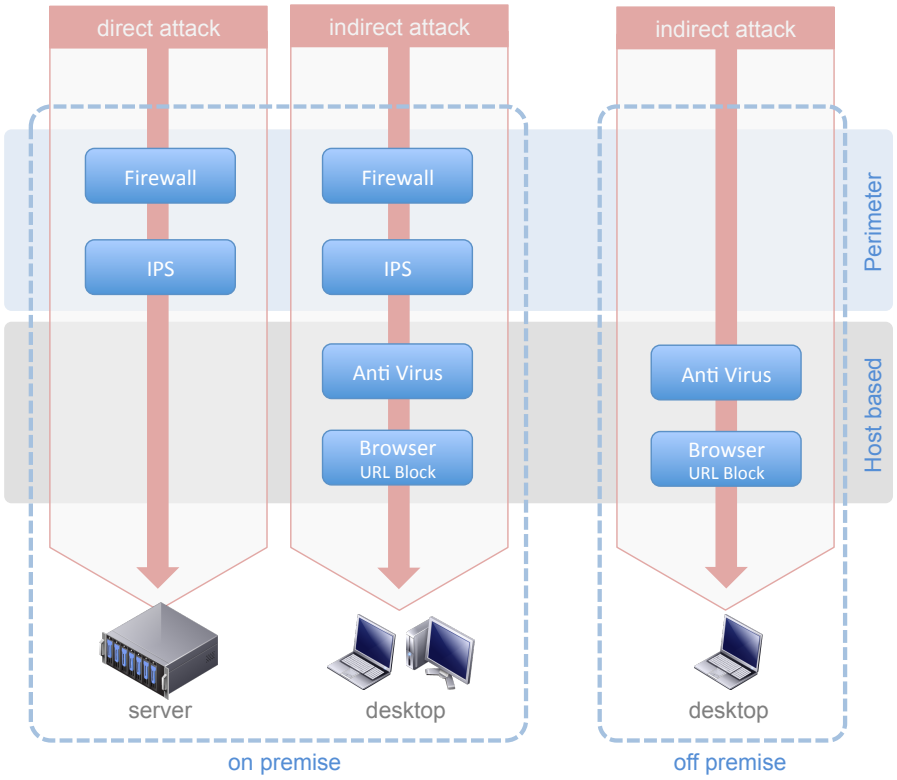

Figure 4 – Intruders Attack Path Options vs. Layers of Defense Technologies

Implementation of multiple layers of diverse defense technologies can be a complex process with multiple factors affecting the overall security effectiveness of the solution. The key challenge for any kind of protection technology is achieving a high block rate while keeping the number of false positives low, paired with stability, reliability, and acceptable performance. An inline security appliance must not degrade network performance or it will never be installed. A high rate of false positives creates considerable management workload and frustrates users and operators alike – this typically results in log entries and reports being ignored, or the device itself being deactivated.

In order to determine the security effectiveness of devices on the market and facilitate accurate comparisons, the following metrics were used:

Test Type / Metric	Description
Exploit Block Performance	Tests are engineered to generate the same types of attack used by modern cyber criminals utilizing multiple commercial, open source and proprietary tools as appropriate. With more than 1,400 exploits, this is the industry's most comprehensive test to date. Prior to testing, all live exploits and payloads have been validated such that • a reverse shell is returned, allowing the attacker to execute arbitrary commands • a malicious payload is installed • a system is rendered unresponsive •
Anti-Evasion Performance	Providing exploit protection without factoring in evasion/obfuscation is misleading. For all exploits, additional test cases are generated for each appropriate evasion technique. The complete list of anti-evasion techniques tested can be found in the appendix.
Performance/Leakage	Frequently there is a trade-off between security effectiveness and performance. Testing ensures that new security protections do not adversely impact performance and that vendors don't take security shortcuts to maintain or improve performance. Product performance is tested based upon the average of three traffic types: 21KB HTTP response traffic, a mix of perimeter traffic common in enterprises, and a mix of internal "core" traffic common in enterprises.
Stability & Reliability	Long-term stability is particularly important for an in-line device, where failure can produce network outages. Tests verify the stability of the device under test (DUT) along with its ability to maintain security effectiveness under normal load and while passing malicious traffic. Products that are not able to sustain legitimate traffic (or which crash) while under hostile attack will not pass.

Multiple products, from market leading vendors, represent each class of technology being tested. The products are subjected to an array of the industry's most rigorous testing procedures, including performance, load and stability checks, tests with live malware, known and unpublished exploits, and diverse evasion techniques.

Security Test Results

A. Network Firewall

Firewall technology is one of the largest and most mature security markets. Firewalls have undergone several stages of development, from early packet filtering and circuit relay firewalls to application layer (proxy based) and dynamic packet filtering firewalls. Throughout their history, however, the goal has been to enforce an access control policy between two networks, and thus should be viewed as an implementation of policy. A firewall is a mechanism used to protect a trusted network from an untrusted network, while allowing authorized communications to pass from one side to the other, thus facilitating secure business use of the Internet. As firewalls will be deployed at critical points in the network, the stability and reliability of a firewall is imperative. In addition, it must not degrade network performance or it will never be installed.

NSS tested six enterprise network firewall products from *Check Point, Cisco, Fortinet, Juniper, Palo Alto Networks*, and *SonicWall* in Q1 2011.[2]

The main findings can be summarized as follows:

- Three of the six products tested crashed when subjected to our stability tests. These kinds of crashes indicate the existence of a vulnerability, which an attacker may be able to exploit in the field given enough time. This lack of resiliency is alarming, especially considering that all three were ICSA Labs and/or Common Criteria certified.
- Performance claims in vendor datasheets are generally grossly overstated. Measuring performance based upon RFC-2544 (UDP) does not provide an accurate representation of how the firewall will perform in live real-world environments.
- Five of the six products failed the TCP Split Handshake test, allowing an external server to reverse the flow of TCP and thereby tricking the firewall into permitting a connection, providing an opening for a crafty attacker to circumvent firewall controls. Within a month, four vendors released patches that successfully remediated this issue.

From an Attacker's Perspective

Firewalls crashing under stability tests, paired with overstated performance claims by vendors, indicate opportunities for denial of service attacks. Longstanding, tried, and field proven technology, such as firewalls, can still fail on basic networking attacks, allowing bypass of the security device. Attacks never expire – security devices must maintain protection for the complete range of attacks, including old attacks and attack methods.

B. Intrusion Prevention System (IPS)

Network intrusion prevention systems (IPS) will continue to play a key role in layered defenses. An essential part of layered security, IPS must be fast, accurate, and easy to deploy and maintain. Designed to identify and block attacks against internal computing assets, a good IPS can provide temporary protection and relief from the

[2] Network Firewall Group Test 2011 - https://www.nsslabs.com/reports/network-firewall-group-test-2011

immediate need to patch affected systems. The IPS must catch sophisticated attacks while producing nearly zero false positives. And it must not degrade network performance or it will never be installed.

In 2012, NSS tested 15 enterprise network intrusion prevention (IPS) products from the ten vendors *Check Point, DELL Sonicwall, FortiGate, HP/TippingPoint, IBM, Juniper, McAfee, Palo Alto, Sourcefire*, and *Stonesoft.*[3]

NSS engineers generated the same types of attacks used by modern cyber criminals, utilizing multiple commercial, open source and proprietary tools as appropriate. With 1,486 live exploits, this is the industry's most comprehensive test to date. With the exception of one product, which had difficulty handling SMB evasions, all of the products tested were able to properly decode, defragment, deobfuscate, and normalize attack traffic. The left pane in Figure 5 shows the exploit block performance of the enterprise network intrusion prevention (IPS) products tested. The performance varies considerably, between 17 and 334 undetected exploits by product were found. The right pane in figure 5 visualizes the fact that the same exploit is often undetected by more than one product. For example, a cybercriminal with the right selection of 29 exploits can bypass five vendors' intrusion prevention systems.

The main findings can be summarized as follows:

- Block protection varied between 77 percent and 98 percent, with most tested devices operating above 90 percent.
- Security effectiveness varied between 60 percent and 99 percent, with most tested devices operating above 91%
- Evasion detection has improved considerably with all but one vendor passing the test. One vendor had stability issues.
- Tuning of the IPS policy makes a difference. Vendor default/recommended policies are designed with performance, not security in mind. Prior to tuning, IPS products blocked considerably fewer attacks – some less than 50 percent.[4]

[3] IPS Comparative Analysis 2012 - https://www.nsslabs.com/reports/ips-comparative-analysis-2012

[4] https://www.nsslabs.com/reports/network-ips-group-test-2010

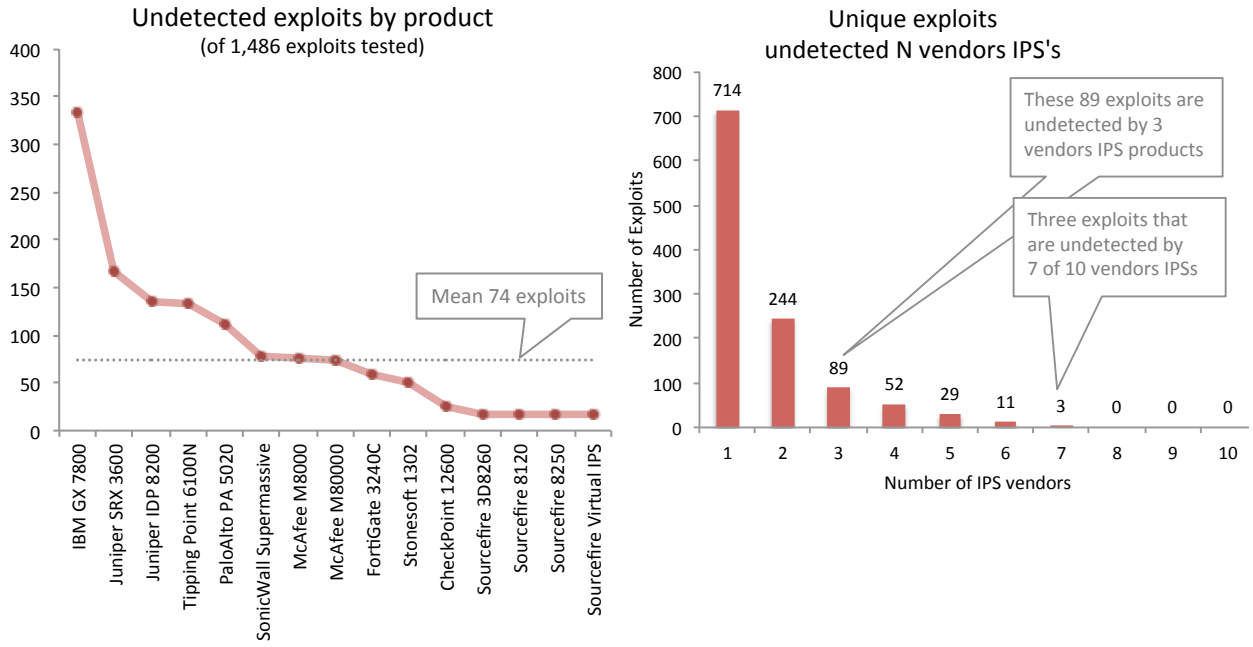

Figure 5 – Number of Undetected Exploits by IPS Product (Left Pane)
Correlation of Undetected Exploits Between Vendors' IPS Products (Right Pane)

From an Attacker's Perspective

None of the devices tested achieved 100 percent block protection. Of the total number of 1,486 exploits tested, one product did not detect 17, for others as many as 334 exploits went undetected. Correlation of undetected exploits with the tested products reveals that only a small set of exploits is required to successfully bypass all IPS products in order to successfully attack prevalent programs or services. The improved evasion detection over previous years demonstrates that independent testing is an effective means to drive vendors to advance their products and remediate weaknesses.

C. Endpoint Protection/Antivirus

The mission of endpoint protection is to defend users against exploits and malware when a patch is not available or has not yet been applied. Users who delay patching, or fail to patch more than their operating system alone, are at elevated risk of compromise. When perimeter protection fails or is not available at all (for example when the user works outside the corporate perimeter), end-point protection is the last line of defense.

In 2012, NSS Labs tested 13 popular endpoint security suites from *Avast, AVG, Avira, ESET, F-Secure, Kaspersky, McAfee, Microsoft, Norman, Norton, Panda, Total Defense*, and *Trend Micro*.[5]

[5] Consumer AV/EPP Comparative Analysis - Exploit Protection - https://www.nsslabs.com/reports/consumer-avepp-comparative-analysis-exploit-protection

These endpoint security suites are tested against 144 exploit attack scenarios to measure their effectiveness in protecting Windows computers against exploits. All of the vulnerabilities exploited during this test have been publicly available for months (if not years) prior to the test, and have also been observed in use on the Internet. Vulnerabilities used in this test were exploited when a user visited an infected web page hosting the attack code. The attacks occurred in two stages:

- The attacker caused a specially crafted stream of data and code to be delivered to a precise location. This exploited the victim's computer, gaining the attacker the ability to perform arbitrary code execution.
- Malicious code was silently executed on the victim's computer.

The main findings are shown in Figure 6 and can be summarized as follows:

- With a few notable exceptions, endpoint products are not providing adequate protection from exploits.
- Antivirus products differ up to 58 percent in effectiveness at stopping exploits, with protection levels varying between 34 percent and 92 percent.
- Many products failed to protect against attacks over HTTPS that were blocked over HTTP, a serious deficiency for a desktop antivirus/host intrusion prevention system.
- Most vendors lack adequate protection against exploits.
- Keeping AV software up-to-date does not yield adequate protection against exploits, as evidenced by coverage gaps for vulnerabilities several years old.

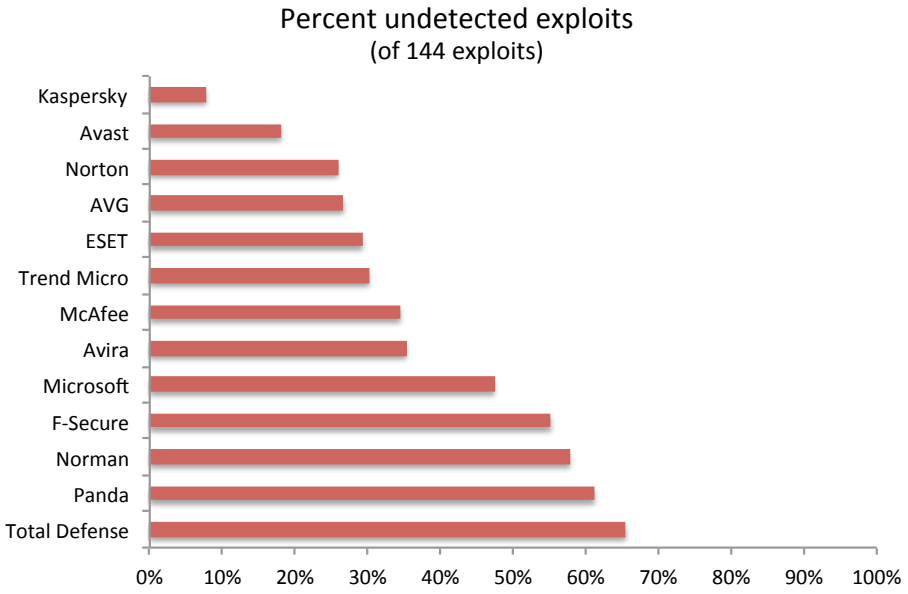

Figure 6 – Endpoint Protection Products – Undetected Exploits

From an Attacker's Perspective

Based on market share, between 65 percent and 75 percent of the world is poorly protected. Most vendors lack adequate protection against exploits and simple evasions like switching from HTTP to HTTPS are often effective in bypassing attack detection. Using recent or old exploits paired with evasion techniques provide an easy road to for attackers to compromise a host. As users are known to only slowly apply security patches, the chances of hitting a

vulnerable target are significant. For example, a typical end-point with the 50 most prevalent programs installed required more that 75 updates in a 12-month period to stay fully patched.[6]

Antivirus does not prevent a dedicated attacker from compromising a target.

D. Browser Blocking

Browsers offer the largest attack surface in most enterprise networks and are the most common vector for malware installations. Web browsers offer a direct and unique route for infection, bypassing corporate protection layers and bringing malware deep into the corporate environment, often protecting it from detection using HTTPS. Browsers must provide a strong layer of defense from malware, rather than defer to operating system antimalware solutions. This capability becomes even more important given the increasing mobility of devices, which means corporate perimeter and network protection services cannot always be relied upon, as shown in figure 4.

In an ongoing campaign using a unique live testing harness, NSS Labs continuously tests the effectiveness of the four leading browsers Microsoft Internet Explorer, Google Chrome, Mozilla Firefox, and Apple Safari to block malware since 2011.[7]

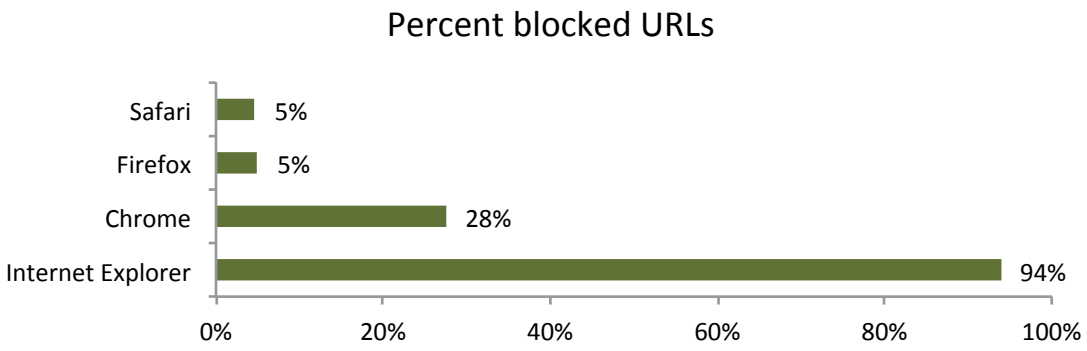

Figure 7 – Overall Malware Block Rate in Test Campaign from December 2011 to May 2012

The main findings can be summarized as follows:

- The use of HTTPS by browsers presents additional problems to organizations since it offers the opportunity to bypass many layers of corporate security protection.
- Internet Explorer maintained a malware block rate of 95 percent while Firefox and Safari's block rate remained just under 6 percent. Over the same time period, Chrome's block rate varied from 13 percent to just over 74 percent.

From an Attacker's Perspective

The tolerance of browsers with low malware block rates may present undue risk to an organization.

[6] The Security Exposure of Software Portfolios
http://secunia.com/?action=fetch&filename=Secunia_RSA_Software_Portfolio_Security_Exposure.pdf

[7] Is Your Browser Putting You At Risk? https://www.nsslabs.com/reports/your-browser-putting-you-risk-part-1-general-malware-blocking

To put the numbers in perspective, for every twenty encounters with socially engineered malware, Firefox and Safari users will be protected from approximately one attack. That means nineteen out of twenty socially engineered malware attacks against Firefox and Safari users will end up testing the user's antivirus and/or operating system defenses. Chrome users will be protected from about six of the twenty attacks, leaving their antivirus and operating systems responsible for protecting against fourteen attacks, and IE10 users will generally be protected from almost all twenty attacks.

Conclusion

Continued security testing of diverse protection products performed over the past decade demonstrates that there is no single technology capable of providing 100 percent protection against modern attacks. There is an ongoing arms race between threat actors and the security industry with continued advances in attack technologies and methodologies. Maintaining pace with cybercriminals is a constant challenge for the industry and, sadly, it is a common occurrence that security products fail to detect older, known, tried and tested attack types, or even fail on device stability. Vendor claims on the security effectiveness or performance of their products are frequently found to be overly optimistic, or based on non-realistic assumptions that do not hold in the field.

Continued independent and real-world testing of security products, and the full and transparent publication of results and failure points, has proven valuable in driving the industry to rectify shortcomings. This test data also serves to inform the users of these products about the limitations in real-world deployments, allowing them to create more accurate risk assessments for their enterprise. It is safe to assume that cybercriminals also thoroughly test existing security technologies to identify shortcomings and exploit them accordingly.

The complexity to secure and control an organizations infrastructure further increases with ongoing adoption of mobile devices (BYOD).

The data presented here, derived from extensive live testing, clearly demonstrates that 100 percent attack prevention is an illusion – more so if you are considered a high value target. Organizations should assume that they are already compromised, and therefore complement prevention with breach detection to identify and act on successful security breaches in a timely manner.

Reading List

The Targeted Persistent Attack (TPA): The Misunderstood Security Threat Every Enterprise Faces. NSS Labs
https://www.nsslabs.com/reports/targeted-persistent-attack-tpa-misunderstood-security-threat-every-enterprise-faces

Top 20 Best Practices to Help Reduce the Threat of the Targeted Persistent Attack. NSS Labs
https://www.nsslabs.com/reports/top-20-best-practices-help-reduce-threat-targeted-persistent-attack

Intrusion Prevention Systems Comparative Analysis. NSS Labs
https://www.nsslabs.com/reports/2012-ips-comparative-analysis

Next Generation Firewall (NGFW) Comparative Analysis. NSS Labs
https://www.nsslabs.com/reports/2012-ngfw-comparative-analysis

Network Firewall Comparative Analysis. NSS Labs
https://www.nsslabs.com/reports/2011-network-firewall-group-test

Consumer AV/EPP Comparative Analysis – Exploit Protection. NSS Labs
https://www.nsslabs.com/reports/2012-consumer-avepp-comparative-analysis-exploit-protection

Browser Security Comparative Analysis: Socially Engineered Malware. NSS Labs
https://www.nsslabs.com/reports/browser-security-comparative-analysis-socially-engineered-malware

Breach Detection: Don't Fall Prey to Targeted Attacks. NSS Labs
https://www.nsslabs.com/reports/breach-detection-dont-fall-prey-targeted-attacks

Appendix

Anti-Evasion Techniques Included in Tests

- IP Packet Fragmentation
- TCP Stream Segmentation
- RPC Fragmentation
- SMB & NetBIOS Evasions
- FTP Evasion
- IP Fragmentation + TCP Segmentation
- IP Fragmentation + MSRPC Fragmentation
- IP Fragmentation + SMB Evasions
- TCP Segmentation + SMB / NETBIOS Evasions
- URL Obfuscation
- HTTP Encoding
- HTTP Compression
- HTML Obfuscation
- Payload Encoding
- Payload Compression & Encoding

Contact Information

NSS Labs, Inc.
206 Wild Basin Rd
Building A, Suite 200
Austin, TX 78746 USA
+1 (512) 961-5300
info@nsslabs.com
www.nsslabs.com

This analyst brief was produced as part of NSS Labs' independent testing information services. Leading products were tested at no cost to the vendor, and NSS Labs received no vendor funding to produce this analyst brief.